Проект «Арт-Шифр»

Ходоровская М.И., ГалатинК.И.
Научный руководитель
Торошилова С. Ю.
МАОУ СОШ №33 г., г. Калининград, Россия

Актуальность проекта

Информационная безопасность приобрела особую значимость в условиях высокого развития интернета и цифровых услуг. Люди ежедневно сталкиваются с необходимостью сохранять конфиденциальность своих данных: банковских счетов, электронных писем, медицинских записей и прочей личной информации.

Проект «Арт-Шифр» направлен на повышение уровня осведомлённости молодёжи о криптографии, развитии навыков критического мышления и умения создавать уникальные механизмы защиты информации. **Основная идея проекта -** создание художественной криптографической системы, в которой сочетаются математика и визуальные образы, что делает процесс шифрования интересным и привлекательным.

Задачи проекта включают:

1. Ознакомление с основами криптографии;
2. Анализ существующих методов шифровки и дешифровки;
3. Разработка оригинального способа шифрования при помощи палитры и картин;
4. Реализация концепции «Арт-Шифра» в виде прикладного программного продукта;

Описание принципа работы шифра

Мы разработали шифр на стыке математики и искусства, который представляет собой оригинальную систему с высокой криптостойкостью для непрофессионального использования. Моя идея заключается в создании специального ключа, где каждой букве алфавита ставятся в соответствие не один, а несколько цветовых оттенков, расположенных друг напротив друга в цветовом круге - такой прием затрудняет частотный анализ и вводит потенциального злоумышленника в заблуждение. Чтобы зашифровать сообщение, мне достаточно этого ключа и любой картины. Процесс шифрования выглядит следующим образом: я смотрю на букву, которую необходимо зашифровать, нахожу на ключе соответствующий ей оттенок на выбранном полотне и вместо буквы записываю точную координату этого фрагмента. Конечное сообщение превращается в набор цифр, расшифровать который может только тот человек, у которого есть оригинальный ключ. Данный шифр особенно актуален для людей, связанных с искусством, поскольку им гораздо проще идентифицировать нужные оттенки, а в их распоряжении обычно имеется целая коллекция картин. Возможность использовать для каждого нового сообщения другое полотно значительно повышает криптостойкость, ведь найти то самое изображение среди бесчисленного множества картин на планете практически невозможно. Даже если третье лицо каким-то образом получит ключ, без знания конкретного полотна процесс дешифровки займет настолько много времени, что исходное сообщение к этому моменту потеряет свою актуальность.

Технология реализации

Решение выполнено в виде программы на языке Python с использованием библиотеки PyQt5. Интерфейс программы удобен и функционален:

- Выбор изображения для шифрования осуществляется посредством встроенного диалогового окна.
- Назначение цветов буквам производится интерактивно — простое щелчок мышью выделяет пиксел на экране и позволяет задать соответствующую букву.
- Процесс шифрования и дешифрации полностью автоматизирован и занимает минимальное время.